
 THE CITY OF DULUTH MINNESOTA	PAYMENT CARD INDUSTRY (PCI) COMPLIANCE POLICY	
	Supersedes:	Date Approved: March 16, 2017
	Approved: 	Page 1 of 3

OVERVIEW	
Objective	All card-processing activities and related technologies must comply with the Payment Card Industry Data Security Standard (PCI-DSS) in its entirety. Card-processing activities must be conducted as described herein and in accordance with the standards and procedures listed in this policy. No activity may be conducted nor any technology employed that might obstruct compliance with any portion of the PCI-DSS.
Policy Statement	<p>The standards are designed to protect cardholder information of patrons that utilize a credit card to transact business with the City of Duluth. This policy is intended to be used in conjunction with the complete PCI-DSS requirements as established and revised by the PCI Security Standards Council.</p> <p>Without adherence to the PCI-DSS standards, the City of Duluth would be put in a position of unnecessary reputational risk and financial liability. Merchant account holders who fail to comply are subject to:</p> <ul style="list-style-type: none"> • Any fines imposed by the payment card industry; • Any additional monetary costs associated with remediation, assessment, forensic analysis, or legal fees; • Suspension of the merchant account.
Scope	<p>All persons who have access to credit card information, including:</p> <ul style="list-style-type: none"> • Every employee that accesses, handles, or maintains credit card information. City of Duluth employees include full-time, part-time, interns, volunteers, and hourly staff members who access, handle, or maintain records; • Employees who contract with service providers (third-party vendors) who process credit card payments on behalf of the City of Duluth; • Information Technology staff responsible for IT security, SAQ completion, and scan review of City of Duluth systems to insure no credit card numbers are stored electronically.
Related Forms	• N/A
Related Policies	• N/A

RESPONSIBILITIES AND EXPECTATIONS
<p>Procedures</p> <p>The City of Duluth requires compliance with PCI standards. To achieve compliance, the following requirements must be met by departments or third party service providers accepting credit cards to process payments on behalf of the City of Duluth.</p> <ul style="list-style-type: none"> • Management and users must be familiar with and adhere to the PCI-DSS requirements of the PCI Security Standards Council. • Employees involved in processing credit card payments must acknowledge (Appendix A) that they have read, understood, and agree to adhere to Information Security policies of the City of Duluth, this policy, and have gone through the required training. • User security must be set to least privilege necessary. • City of Duluth Auditor must approve each merchant bank or third-party vendor that is to engage in the processing or storage of transaction data on behalf of the City of Duluth—regardless of the manner or duration of such activities. <p>Data Storage and Disposal</p> <ul style="list-style-type: none"> • Credit card information must NOT be entered/stored on paper or electronically on the City of Duluth network servers, workstations, laptops, removable media, or mobile devices.

- Credit card information must NOT be transmitted via email, fax, or IM/Chat tools.
- Web payments must be processed using a PCI-compliant service provider approved by the City of Duluth Auditor and IT management.
- Electronic storage of credit card data is prohibited by this policy; the City of Duluth may perform a quarterly network scan to ensure that the policy has not been violated.
- Any paper documents containing credit card information should be limited to information required to transact business, only those individuals who have a business need to have access, should be in a secure location, and must be destroyed via approved methods once business needs no longer require retention.
- All credit card processing machines must be programmed to printout only the last four or first six characters of a credit card number.
- Neither the full contents of any track for the magnetic strip nor the three-digit card validation code may be stored in a database, log file, or point of sale product.
- Transmission of any credit card information must be encrypted.

If you are a user who processes credit cards...

- Ensure both the customer receipt and your merchant receipt does not include the full account number or expiration date.
- Make sure you have anti-virus and anti-malware programs installed on any computer system that contains your payment applications and are updated regularly.
- Change any IDs and passwords supplied by the payment application vendor to ones that are unique and complex in nature.
- Use a unique ID and password that is complex in nature for every employee accessing the computer system and/or the payment application.
- If you have vendors that access your computer systems remotely, ensure they are using secure access protocols and you are monitoring any activity they are performing.
- Do not store the three-digit number on the back of payment cards (CVV2) in any format.
- Do not request the CVV2 number on mail-order forms or billing forms.
- Examine card swipe devices at least monthly to look for any sign of tampering.
- Verify the identity of any third-party persons claiming to be repair or maintenance personnel prior to granting them access to modify or troubleshoot devices.
- Immediately document and report to management any suspected or actual security incidents.

Training

- All users who access, handle or maintain credit card information and their managers will be required to complete training on PCI compliance and acknowledge their understanding of the training and this policy on an annual basis.

Enforcement

IT will oversee enforcement of this policy, lead investigations about credit card security breaches and may terminate access to protected information of any users who fail to comply with this policy.

Payment Card Industry (PCI) Compliance Policy

Appendix A – Acknowledgement Summary

City of Duluth employees working with credit cards must read and understand the following:

- Approval must be obtained from the City Auditor and IT management before entering into any contracts or purchases of software and/or equipment related to credit card processing. This requirement applies regardless of the transaction method or technology used (e.g., e-commerce, POS device).
- The Department and all its employees must comply with the Payment Card Industry Data Security Standard.
- Departmental procedures must be established for safeguarding cardholder information and secure storage of data. This pertains to ALL transactions initiated via the telephone, over the counter, mail order, Internet, etc.
- Credit card numbers must not be transmitted in an insecure manner, such as by email, instant messaging, unsecured or stored fax, or through City mail (sealed envelopes must be used).
- Cardholder data (i.e., full account number, card type, expiration, PIN, and card-validation code [three-digit or four-digit value printed on the front or back of the card]) should not be stored on paper or in any electronic format.
- The entire credit card number must not be printed on either the department copy or customer copy of any receipts. Do not print the full credit card number under any circumstances.
- All documentation containing card account numbers must be stored in a secure environment until processed. Secure environments include locked drawers and safes, with limited access to only individuals who are processing the credit card transaction. Processing should be done as soon as possible and the credit card number should immediately be shredded.
- No employee shall disclose or acquire any information concerning a cardholder's account without the cardholder's consent.
- All employees including their managers that access, handle or maintain credit card transactions must complete required card security training annually.
- Vendor-supplied default system passwords will be changed or disabled immediately upon system implementation.